Storage Infrastructure will consist of Highly Available SAN devices and fiber switches are recommended for connectivity. Windows servers will access the SAN via Fiber Channel Host Bus Adapter (HBA). A secondary fiber switch is recommended for High Availability access to the SAN.

Fiber Channel connectivity should use 2 to 4 gigabyte speeds with channeling as an option. Switch ports should be configured with access control lists for only allowed traffic. Logical Unit Number (LUN) should be configured to allow only needed MAC address access. Dual HBA's should be used for each Windows server for load balancing and failover capabilities.

The SAN should be installed and configured with assistance from vendor Engineers. Vendor SAN software for management and monitoring is preferred to ensure optimum available and security.

Table 3 Drive matrix

Data Type	Drive Recommendation	Explanation
Archive Data	ATA or SATA	Low cost drives with high storage capabilities. Archive environment is mostly read only data and rarely accessed. Access speed is not important
Core Data	15K drives Fiber Channel Drives	High read and write requirements
Processing Data	10K large Fiber Channel Drives	Average read/write requirements

1.8 Authentication and Authorization Infrastructure

For MEUPS to control applications they need to be claims aware following the WS-* Web Services Architecture. This standard is cross platform allowing for applications to be secured across enterprise boundaries. Active Directory Federation Services will facilitate authentication and authorization between each application and the controlling directory service.

MEUPS uses a single Active Directory forest/domain model called **GAMMIS** which will be the primary controller of authentication for the first phase of applications. MEUPS will use this directory service for all account provisioning until another directory service is instituted. MEUPS was designed to integrate with multiple account stores, but due to network and project complexities the directory structure was reduced to a single Active Directory configuration. MEUPS applications will forward login requests to an ADFS server which will then authenticate against **GAMMIS** Active Directory. All user accounts will be provisioned through the MEUPS web UI. Once the accounts are created in MEUPS they will be synchronized into **GAMMIS** Active Directory. Once this process has happened, a user may access the applications in which they have been granted rights or roles to. The account synchronizer process runs in real time will an average account created/updated within minutes of submitting the request through MEUPS. MEUPS and ADFS will define and control access via 'claims' for all applications. Application roles are first defined within MEUPS for each application then mapped to an Active Directory global security group. When an application is published in MEUPS security roles should be populated at that time. Security roles define the application access such as an administrator, super user or agent. For each application, a separate security group will be created in Active Directory when an associated Active Directory Sync Group Name (ADSyncGroupName) is provided. MEUPS provides a graphical interface to manage application security roles. Users defined or created with MEUPS can be added or removed from these security roles through the MEUPS UI.

Security roles or ADFS claims will follow a basic naming standard of *CompanyInitials_AppInitials_ClaimName*. The use and purpose of application ADFS claims will be administrated by EDS. Application will only receive ADFS claims approved by EDS. ADFS will be configured to perform a *group extraction* for each user login which will be mapped to a specific application ADFS claim. This is a supported process between ADFS and Active Directory for mapping users to application ADFS claims. Custom ADFS Claims that cannot be mapped to a security group for any reason can use the Custom Claim Transform Module (CCTM). The CCTM will provide custom ADFS claims where security group membership is not extensible enough for application access control. These custom ADFS claims will follow the same naming standard as regular ADFS claims but will be generated from MEUPS as part of the ADFS and Active Directory authentication process. The MEUPS database will store custom ADFS claims and the business logic to determine which ADFS claims a user should receive during the ADFS login. Custom ADFS claims will be administrated by EDS and application developers can request custom ADFS claims from EDS as needed.